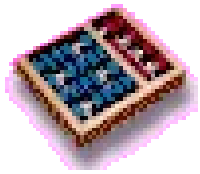


Wireless Security

Rogério Esteves Salustiano

Tiago Nunes dos Santos

♦ Agenda

- Conceitos
- Mecanismos de Segurança
- Riscos
- Ataque x Defesa
- Ferramentas de ataque/escuta/monitoramento de redes sem fio
- Padrões e Tecnologias
  - > Bluetooth
  - > GSM
  - > IEEE 802.16
- Conclusões

♦ Conceitos

Fundamentos

- Cabo X Ar: proteção dos dados, alcance
- Freqüências: Alcance

  PS = 32.4 + (20 log D) + (20 log F)

- Canais: proximidade pode gerar interferências
- *Spread Spectrum*: Maior consumo de banda
  Monitoramento apenas vê “ruídos”
- FHSS: Freqüência alterada regularmente
  Velocidade de transmissão máxima de 2Mbps
- OFDM: Modulação de sinal e isolamento de freqüências

♦ Conceitos

Fundamentos

- Bandas de radiofreqüência públicas
  * 2,4 Ghz
  * 5 Ghz
  * Freqüências Licenciadas

- BEACON *Frames* (ESSID): públicos ou conhecido dos clientes

- Meio compartilhado

- Redes *Ad-hoc*: ausência de um responsável pela segurança

- Redes Infra-estruturadas: único ponto de falha

♦ Mecanismos de Segurança

- Endereçamento MAC
- WEP
- WPA
  * Criptografia
  * EAP
- Autenticação

♦ Mecanismos de Segurança

Endereçamento MAC

- Endereçamento universal único
  * Placas antigas

- Cadastramento prévio da MAC cliente

- Custo de manutenção
  * Redes menores
  * Poucas mudanças

- Direção inversa: MAC do concentrador
  * Conectar ao concentrador correto

♦ Mecanismos de Segurança

Wired Equivalent Privacy (WEP)

- Protocolo de criptografia mais popular em dispositivos wi-fi

- Algoritmos simétricos → Chave secreta compartilhada

- Motivos para a adoção
  * É suficientemente forte
  * Implementa auto-sincronismo
  * Requer poucos recursos computacionais
  * É exportável internacionalmente
  * De uso opcional

- Direção inversa: MAC do concentrador
  * Conectar ao concentrador correto

♦ Mecanismos de Segurança

Wired Equivalent Privacy (WEP) - Chaves

- Chave Completa = Chave Dinâmica + Chave Pública

- Chave Dinâmica = Vetor de Inicialização (VI)
  * Tamanho: 0 a 24 bits

- Chave Pública = Registrada manualmente
  * De 40 a 64 bits
  * Implementações de 128 bits
    + 104 a 128 bits

- *Payload* = *Frame Body* + ICV

- Chave Pública de tamanho máximo
  * Comumente usada
  * Parte da Chave Completa não passa em claro na rede
  * Manutenção da Chave Pública

♦ Mecanismos de Segurança

Wired Equivalent Privacy (WEP) - Chaves

- Chave Pública passa por um módulo RC4
  * São geradas 4 chaves pelo algoritmo
  * Apenas uma delas será utilizada

- Dados cifrados = *Payload* XOR (VI + resultado-RC4)

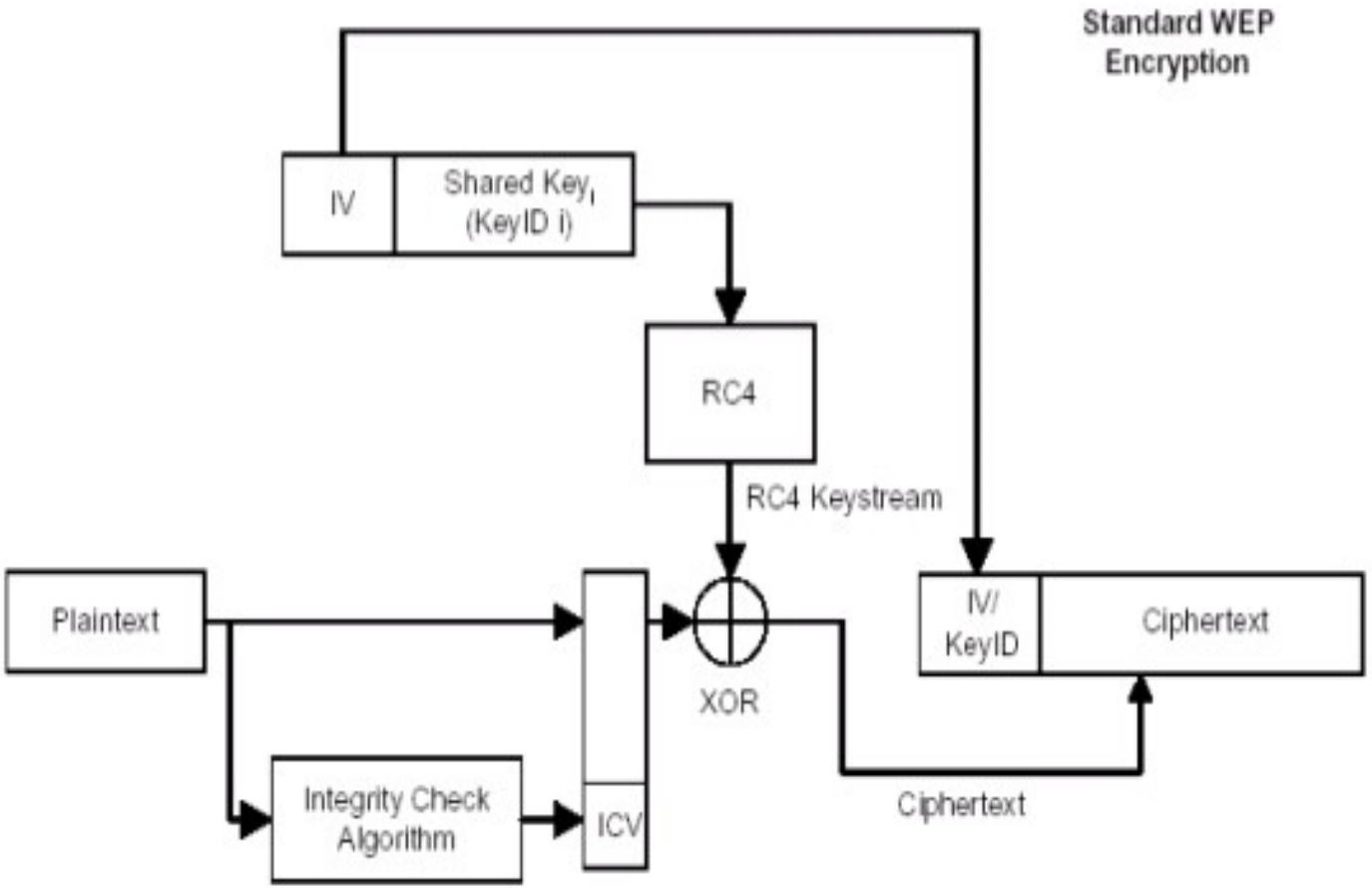
- *Frame* a ser enviado é composto por:
  * VI (em claro)
  * ID da chave resultado-RC4 utilizada (em claro)
  * *Payload* (cifrado)

- Decriptação:
  * VI recebido
  * Calculo do RC4, aplicação do ID recebido
  * *Payload* cifrado

- Duração da criptografia é o processo de transferência

♦ Mecanismos de Segurança

Wired Equivalent Privacy (WEP) - Chaves



♦ Mecanismos de Segurança

Wired Equivalent Privacy (WEP) - VI

- É um vetor gerado (pseudo)aleatoriamente :)

- RC4
  * Recebe uma semente K (de 1 a 2048 bits)
  * A partir de K, gera um vetor S de 256 bytes
    + Posições permutadas, de acordo com K
  * Dados do vetor são utilizados para criar uma seqüência de números pseudo-aleatórios

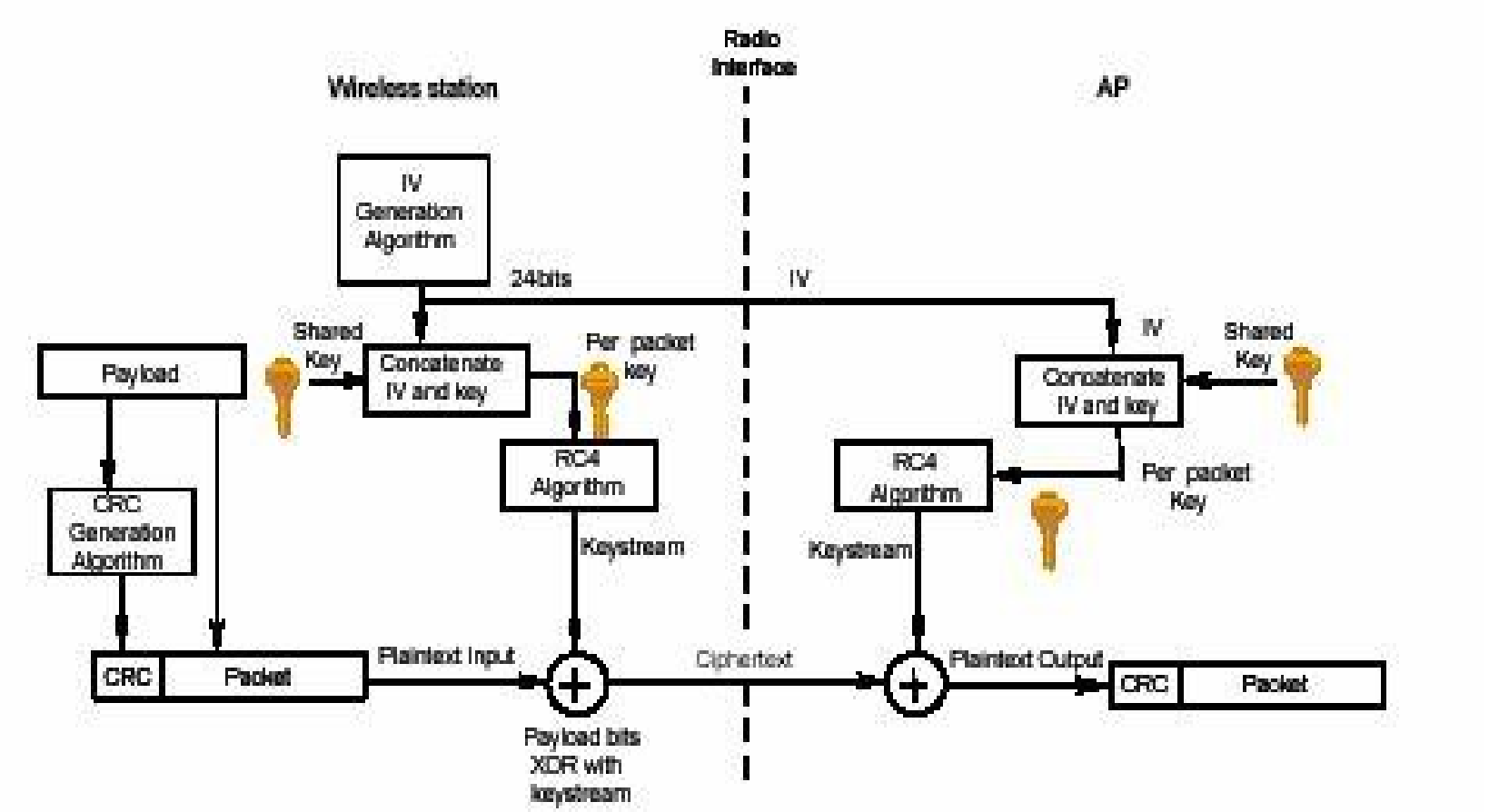
- K = VI concatenado à Chave Pública

- PRNG é o algoritmo gerador de números pseudo-aleatórios do RC4

- KSA é o algoritmo utilizado para permutar o vetor S gerado

♦ Mecanismos de Segurança

Wired Equivalent Privacy (WEP) - VI



♦ Mecanismos de Segurança

Wired Equivalent Privacy (WEP) - VI

- PRNG = Pseudo Random Number Generator

http://www.ppgia.pucpr.br/~maziero/pesquisa/ceseg/wseg03/07.pdf

http://www.gnu.org/software/gnu-crypto/manual/api/gnu/crypto/prng/package-summary.html

http://www.codeproject.com/cpp/xor256stream.asp

http://igbt.sel.eesc.sc.usp.br/cgi-bin/dwww?type=file&location=/usr/share/doc/libsasl2/draft-burdis-cat-srp-sasl-08.txt

http://world.std.com/~cme/P1363/ranno.html

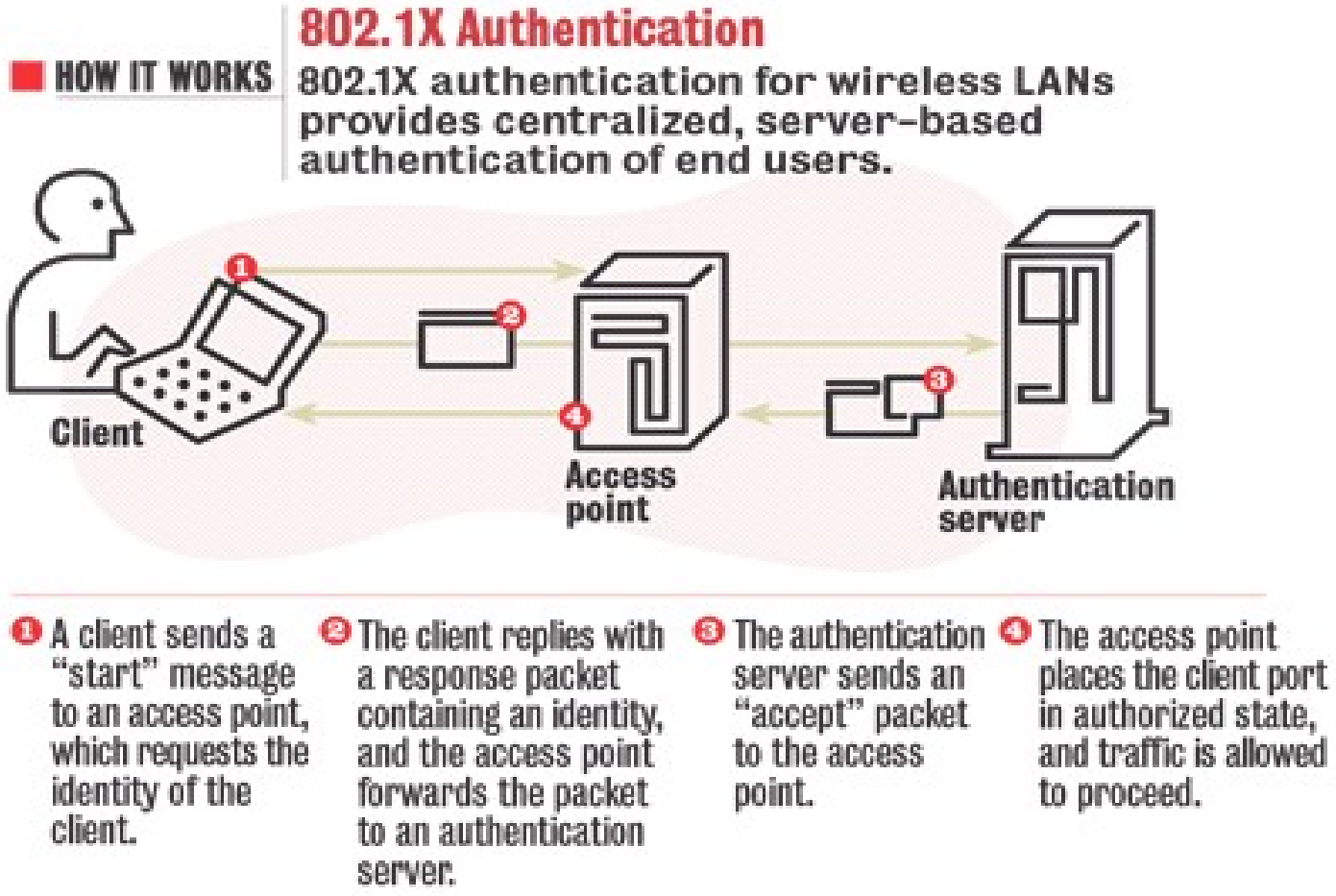
♦ Mecanismos de Segurança

Wi-fi Protected Access (WPA)

- Problemas de segurança com o WEP
- Faz parte do IEEE 802.11i
- Sem suporte a conexões ad hoc
- Atuação:
  * Criptografia dos dados
  * Autenticação do usuário
    + IEEE 802.1x
    + Extensible Authentication Protocol (EAP)

♦ Mecanismos de Segurança

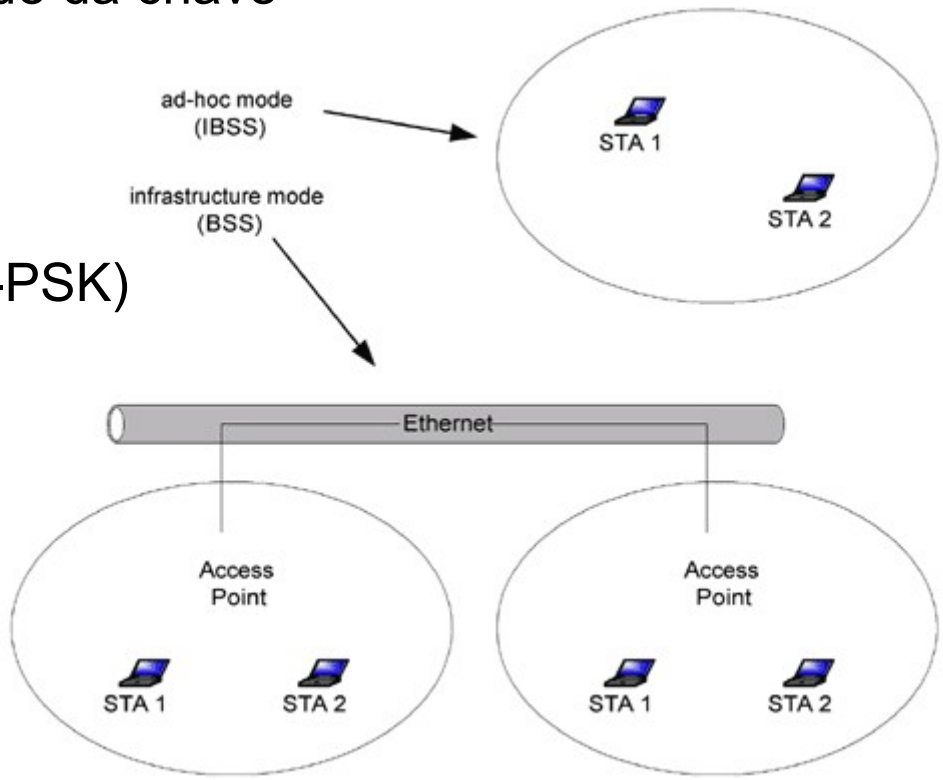
Wi-fi Protected Access (WPA)



♦ Mecanismos de Segurança

Wi-fi Protected Access (WPA) - Criptografia

- Algoritmos + Temporalidade da chave
- Versatilidade
- Pequenas redes
  * *Pre-shared Key* (WPA-PSK)
- Infra-estruturada:
  * Servidor RADIUS
  * ICP quando usados certificados digitais



♦ Mecanismos de Segurança

Wi-fi Protected Access (WPA) - Criptografia

- Chave compartilhada
  * Funciona em ambientes restritos
  * Nenhum problema conhecido (divulgado) com WPA-PSK

- Troca dinâmica de chaves
  * *Temporal Key Integrity Protocol* (TKIP)
    + Transferência da chave mesclada ao pacote
    + Checagem da integridade
    + Mecanismo gerador de nova chave
    + Aumento do VI – 48 bits
    + Alteração do VI por pacote, sessão ou período
  * CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*)
    + AES (Advanced Encryption Standard)
    + WPA + Gerência de Chaves + Integridade da chave

♦ Mecanismos de Segurança

Wi-fi Protected Access (WPA) - EAP

- Extensible Authentication Protocol

- Framework de autenticação
  * Funções comuns e métodos de negociação
  * Possui aproximadamente 40 métodos implementados

- Implementado oficialmente pelo WPA

- Versatilidade
  * Ambientes mistos: cabos + redes → base única de autenticação

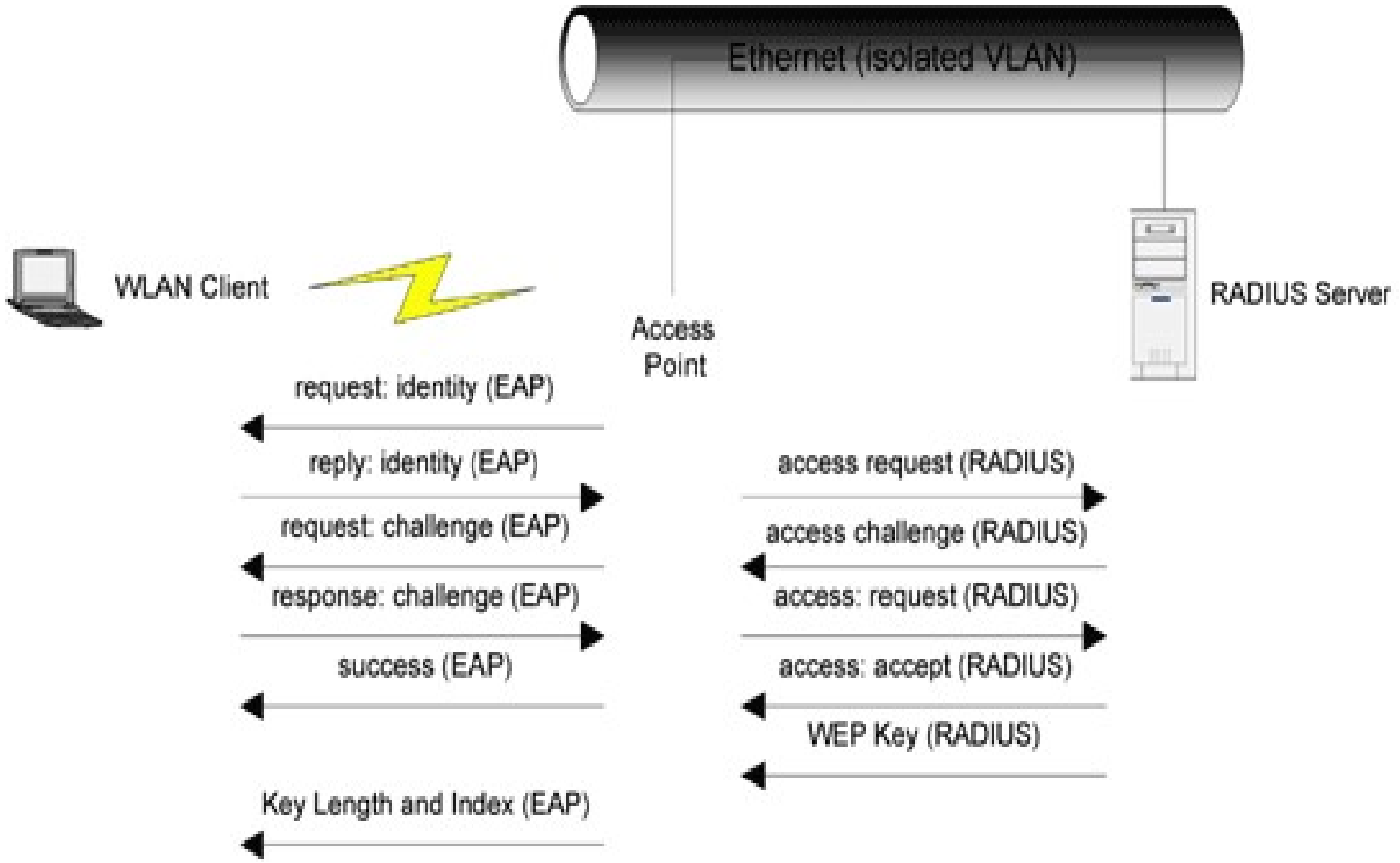
♦ Mecanismos de Segurança

Autenticação

- Utiliza o servidor RADIUS - RFC 2865 e 2866 atualmente
  * RFC 2058 e 2059 de 1997
- RADIUS = Remote Authentication Dial In User Service
- Dupla user/password
- Coordenação das sessões dos usuários
- Utiliza o SNMP para monitoramento remoto

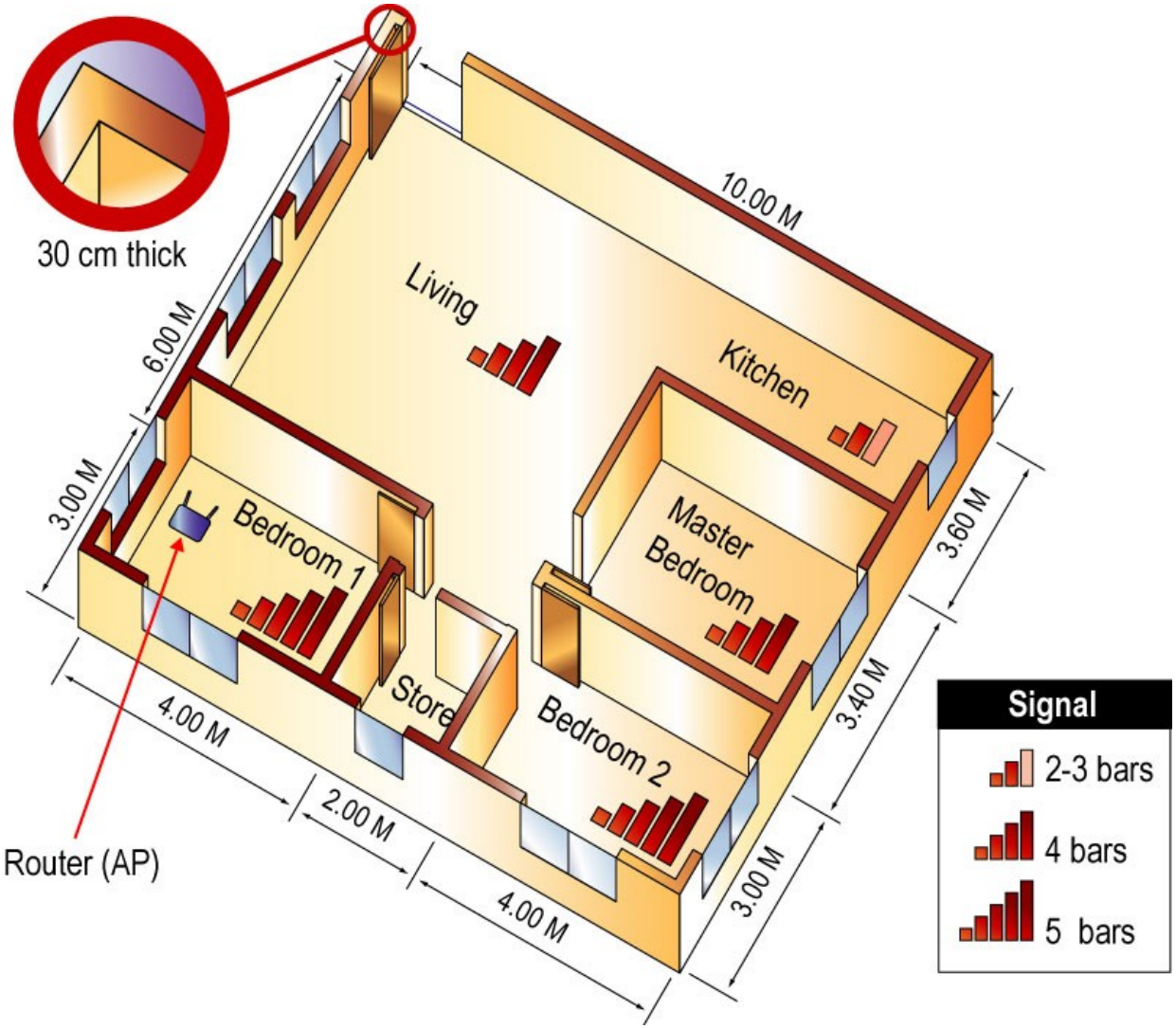
♦ Mecanismos de Segurança

Autenticação

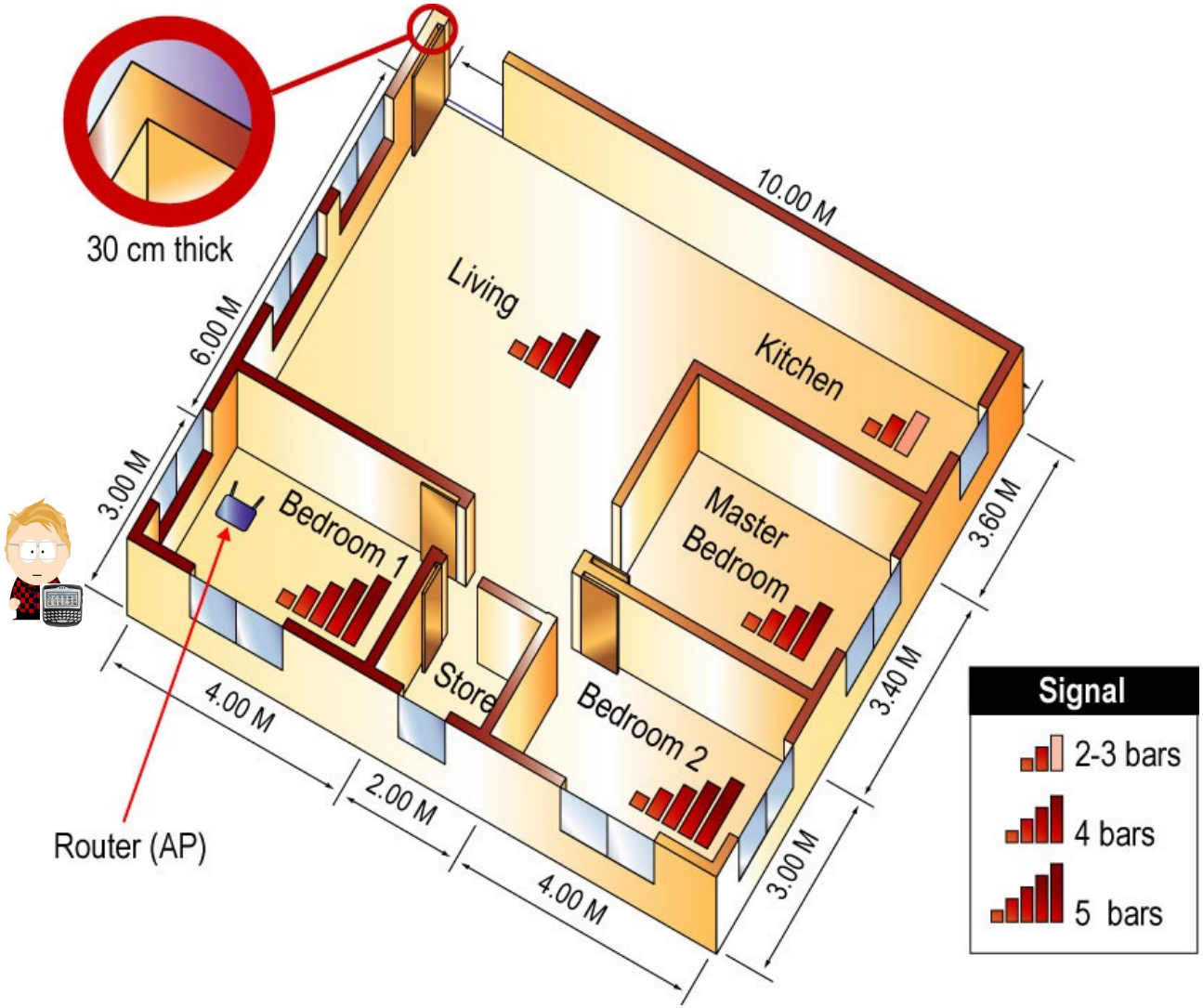


♦ Ameaças

♦ Ameaças


30 cm thick
10.00 M
6.00 M
3.00 M
Living
Kitchen
Bedroom 1
Master Bedroom
Store
Bedroom 2
3.60 M
3.40 M
3.00 M
4.00 M
2.00 M
4.00 M
Router (AP)
Signal
2-3 bars
4 bars
5 bars

♦ Ameaças


30 cm thick
10.00 M
6.00 M
3.00 M
Living
Kitchen
Bedroom 1
Master Bedroom
Store
Bedroom 2
3.60 M
3.40 M
3.00 M
4.00 M
2.00 M
4.00 M
Router (AP)
Signal
2-3 bars
4 bars
5 bars

♦ Ameaças

- Segurança física
  * Área externa do prédio
  * Padrão a ser adotado
  * Potência das antenas

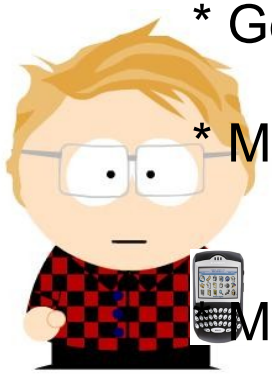
- Configurações *default*
  * Senha do *root*
  * Chaves WEP

- Envio e recepção do sinal
  * Posicionamento central dos concentradores

- Ataques de *Denial of Service* (DoS)
  * Bluetooth classe 1 e 802.11g baixa velocidade, por exemplo

♦ Ameaças

- Mapeamento do Ambiente
  * Mapeamento passivo
  * Geração de mapas (com GPS)
    + Softwares como GPSD, Kismet, Gpsmap, Gpsdrive
  * Mapeamento ativo
    + MAC → Fabricante → Vulnerabilidades conhecidas
    + THC-rut, nmap
  * Mapeamentos em camadas de baixo nível
    + TCPdump. Exemplo:



```
08:40:41.213128 Beacon (OMITIDO) [2.0* Mbit] ESS Ch: 1
08:40:41.297159 Authentication (Open System)-1: Sucessful
08:40:41.297415 Acknowledgment RA:00:0d:9d:c6:5c:34
```

♦ Ameaças

- Captura do tráfego
  * Ferramentas tradicionais

- Acesso não autorizado a configurações básicas
  * Configuração aberta
  * Configuração fechada
    + SSID

- Equipamentos cabeados e sem fio interagindo
  * Wi-fi em modo *ad-hoc*

♦ Ameaças

- Vulnerabilidades em WEP e WPA

- WEP
  * Compartilhamento da chave pública
  * Algoritmo RC4 revela o tamanho da mensagem original
  * Vetor de iniciação

♦ Ameaças

- Vulnerabilidades em WEP e WPA

- WEP
  - * Compartilhamento da chave pública
  - * Algoritmo RC4 revela o tamanho da mensagem original
  - * Vetor de iniciação
    - + As contas

```
24 bits → 16.777.216 combinações
600 pacotes/s transmite em média uma rede
600x60x60 = 2.160.000 pacotes por hora
8 horas → 17.280.000 pacotes ou combinações
```

♦ Ameaças

- Vulnerabilidades em WEP e WPA

- WEP
  * Compartilhamento da chave pública
  * Algoritmo RC4 revela o tamanho da mensagem original
  * Vetor de iniciação
    + As contas

```
24 bits → 16.777.216 combinações
600 pacotes/s transmite em média uma rede
600x60x60 = 2.160.000 pacotes por hora
8 horas → 17.280.000 pacotes ou combinações
```

♦ Ameaças

- Vulnerabilidades em WEP e WPA

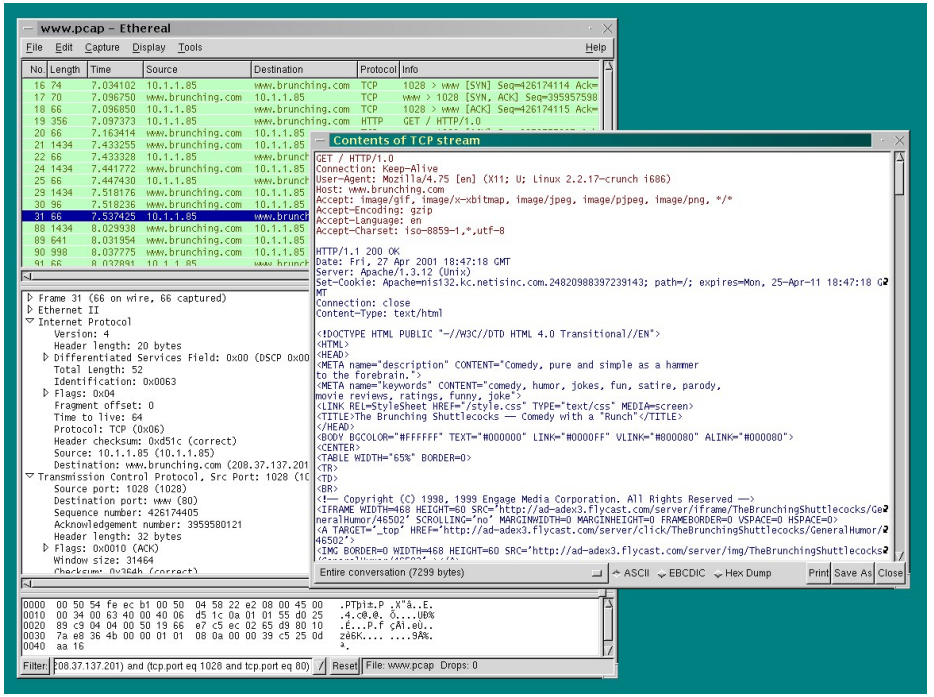
- WEP
  * ping → ICMP_Reply → XOR
  * Sequência de IV a partir do boot do concentrador
  * Armazenamento da chave no cliente é limpa

- WPA
  * Força Bruta + Dicionário de senhas (padrão principalmente)
  * Busca de chaves compartilhadas
  * Problemas no armazenamento da chave

♦ *Técnicas de ataque/escuta*

- ***Escuta de tráfego***

- Sempre é possível obter informações sobre uma rede caso o tráfego esteja aberto, ou seja, sem nenhum mecanismo criptográfico envolvido. Um simples ***tcpdump*** pode ser utilizado. Outras ferramentas como o ***Ethereal*** podem ser utilizadas para o mesmo fim.



Telas do Ethereal: Escuta de tráfego

♦ *Técnicas de ataque/escuta*

• ***Endereçamento MAC***

- O endereço MAC é único em cada dispositivo da rede, contudo uma estação clandestina pode facilmente alterar seu endereço MAC para se fazer passar pela estação legítima. Pode-se ainda, travar a estação legítima e assumir a identidade do concentrador.

Procedimento:

1) Capturar o endereço MAC do concentrador através de Escuta de Tráfego;

2) Alterar o MAC da estação clandestina para o mesmo da estação legítima. Isso pode ser realizado através do comando **ifconfig** (Linux/Unix) ou **etherchange** (Windows).

♦ *Técnicas de ataque/escuta*

• ***Ataques do tipo "homem no meio"***

- Em redes sem fio há um elemento chave onde a interceptação pode ser realiza: o concentrador.

- As ferramentas **AirJack** e **AirSnarf** são capazer de automatizar o processo de ataque "homem no meio".

• ***Quebra de chaves WEP***

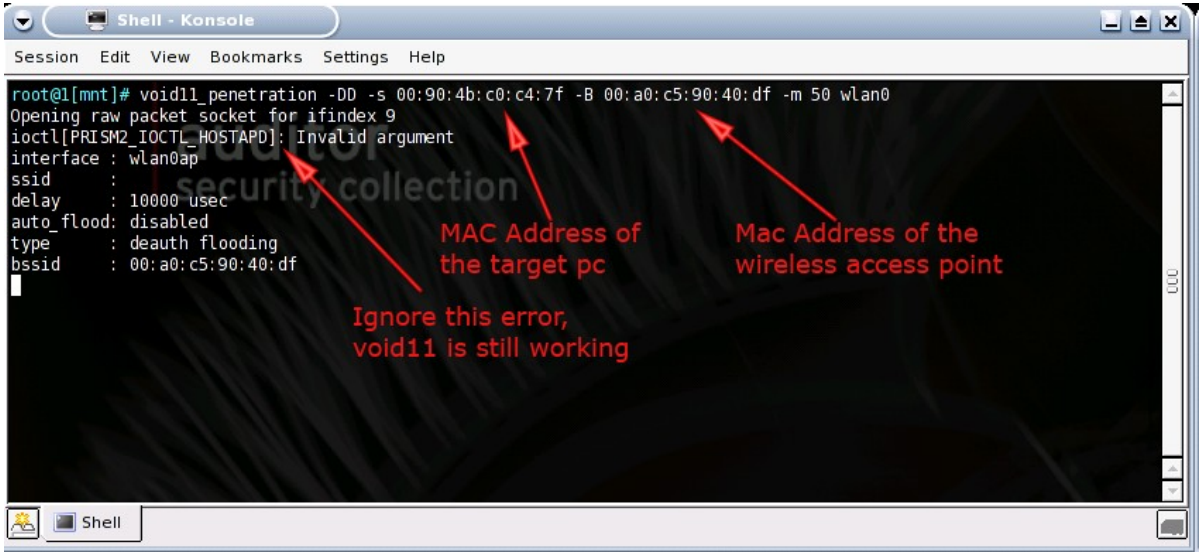
- As ferramentas **Airnort, WebCrack, WepAttack, Wep-tools, Weplab** e **AirCrack** implementam algoritmos para tentativa de quebra das chaves WEP. Em geral utilizam uma combinação de força bruta, ataques baseados em dicionários e exploração de vulnerabilidades conhecidas (chave única, estática e compartilhada por todos os dispositivos participantes de uma determinada rede por exemplo).

♦ *Técnicas de ataque/escuta*

- ***Negação de serviço (DoS)***

- Em geral necessita de grande quantidade de banda para atingir o objetivo, mas em redes sem fio ataques de Negação de Serviço podem ser disparados com poucos recursos e muita eficácia.

- Métodos como associação, autenticação ou dissociação em massa podem ser utilizados para esse fim. As ferramentas **Void11** e **Hostapd** implementam esses métodos em conjunto.



Tela do Void11: Ataque de DoS

♦ Técnicas de defesa

• ***Configurações do concentrador***

- concentrador: ponto crítico na arquitetura sem fio.

- geralmente estabelece uma “ponte” entre a rede sem fio e a cabeada, necessitando proteção de ambos os lados.

Precauções:

1) Desabilitar a difusão do envio do SSID

2) Modificar o nome SSID-padrão

3) Substituição do endereço MAC

4) Desabilitar acessos ao concentrador via rede sem fio

5) Ignorar clientes que enviam o SSID igual a “ANY”

6) Cuidados na escolha das chaves WEP

7) Utilizar o concentrador em modo ponto (*bridge*), ou seja, o concentrador não possui endereço IP, impossibilitando o acesso remoto ao equipamento.

8) Desabilitar comunicação entre clientes (PSPF – Publicly Secure Packet Forwarding), ou seja, bloquear o acesso de um cliente a outros ligados ao mesmo concentrador.

♦ *Técnicas de defesa*

- ***Configurações dos clientes***

  - Implementação de Métodos de Autenticação (ex: protocolo RADIUS)

  - Adoção de chaves WEP

- ***VPNs***

  - utilização de VPNs fim a fim e não somente na área cabeada

- ***Uso de criptografia***

  - senhas descartáveis (One-time Password – OTP)

  - uso da certificação digital

- **Detecção de ataques = Monitoramento**

  - utilização de ferramentas como **Widz, wIDS, Garuda, AirIDS, Kismet** ou **Snort-Wireless** para monitora as atividades de uma rede sem fio.

♦ *Ferramentas de ataque/escuta/monitoramento*

• ***Airtraf***

- detecta número de clientes conectados, serviços utilizados e várias totalizações dos dados de envio da rede em tempo real.

- suporta as placas/chipsets: Orinoco/Proxim, Prism2/Hostap e Aronet/Cisco.

• ***Airnort***

- identifica o SSID (identificador único da rede sem fio) e endereço MAC.

- verifica o uso ou não de WEP na rede.

- possibilita a varredura de todos os canais da rede ou de apenas de um canal de interesse.

• ***BSD AirTools***

- permite monitorar o tráfego e capturar pacotes com o objetivo de quebrar chaves WEP.

- só mapeia (através da incorporação de GPS ao sistema) redes 802.11b

♦ *Ferramentas de ataque/escuta/monitoramento*

- ***Netstumbler***

  - permite integração com GPS para mapear a rede.

  - permite identificar redes 802.11 a/b/g

  - não permite capturar tráfego e quebrar chaves WEP

  - apresenta versão para Windows CE

- **Kismet/GKismet**

  - faz o mapeamento da rede (concentradores e redes *Ad-Hoc*) através da integração com GPS.

  - faz a captura de tráfego.

  - é bastante utilizado para o monitoramento das redes

- **FakeAP**

  - é um programa em *perl*

  - recebe conexões de um canal específico

  - utiliza um SSID específico que deve ser conhecido *a priori*

♦ *Ferramentas de ataque/escuta/monitoramento*

• **FakeAP (*continuação*)**

- permite a utilização de uma chave WEP específica

- permite configurar a potência de saída.

• **AirJack**

- ferramenta que permite se “fazer passar” por um contentrador

- permite com facilidade um ataque do tipo “homem do meio” com HTTPS, apresentando um certificado falso e torcendo para que o usuário o aceite sem questionamentos.

• **Airsnarf**

- capaz de simular um concentrador apenas informando o nome da rede (SSID) e redirecionar o tráfego HTTP e DNS.

♦ *Ferramentas de ataque/escuta/monitoramento*

- **Hotspotter**

  - forja um concentrador, forçando que os clientes se conectem à ele.

- **Wellenreiter I e II**

  - faz identificação de redes e clientes conectados

  - verifica o uso ou não do WEP

  - possibilidade de integração com GPS para mapeamento da rede

  - pode ser rodada em PDAs (Zaurus, por exemplo)

  - passa desapercebida pela maioria dos detectores de programas de varredura

♦ Modelo de Segurança Bluetooth

- ***Três modos de segurança***

  Modo 1: sem segurança
  Modo 2: segurança no nível de serviço
  Modo 3: segurança no nível de conexão

  - Os modos de segurança disponíveis nos dispositivos são determinados pelos fabricantes.

  - Dificuldade no ataque: necessidade de proximidade dos dispositos devido à arquitetura da rede *Bluetooth.*

- ***Alguns exemplos conhecidos de ataques***

  - ***Bluejacking***: envio de cartões de visita para telefones com *bluetooth* com mensagens mascaradas, isto é, são enviados dados além do nome e telefone;

  - ***Bluesnarfing****:* tipo de invasão que permite o envio de SMS, efetuação de ligações telefonicas sem o conhecimento e alerta do dono do aparelho telefônico;

  - **Bluebugging**: invasão à agenda telefônica, imagens e outros dados dos telefones com *bluetooth*.

  - ***Car Whisperer***: invasão de dispositivos instalados em carros com o intuito de copiar músicas, transmitir voz para o sistema de áudio o carro, etc;

  - ***Jaimming***: geração de ruído com o intuito de não permitir ou dificultar a comunicação em um determinado ambiente.

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- ***O sistema GSM fornece três serviços de segurança:***

1) Identidades temporárias (confidencialidade da identidade do usuário)
2) Autenticação (identificação do usuário)
3) Ciframento (confidencialidade dos dados do usuário)

O sistema GSM não permite que o SIM autentique a rede.

- ***(1) Identidades Temporárias***

- o IMSI (Identificador Internacional do Assinante Móvel) não é enviado para a Rede GSM e sim um identificador temporário (TMSI – Identificação Temporária do Assinante Móvel).

- o TMSI consiste de apenas 5 dígitos, mas dentro de uma área o usuário é identificado unicamente. Para isso, o código LAI (Identidade de Localização de Área), que identifica a área onde o MS (Estação Móvel) se encontra, é utilizado em conjunto com o TMSI.

Objetivo das Identidades Temporárias:

- não permitir que um invasor tenha a possibilidade de relacionar o usuário com o início de uma requisição de sessão na Rede GSM.

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- ***(2) Autenticação do Assinante***

  - nada mais é do que a verificação da identidade do Módulo de Identificação do Assinante (SIM)

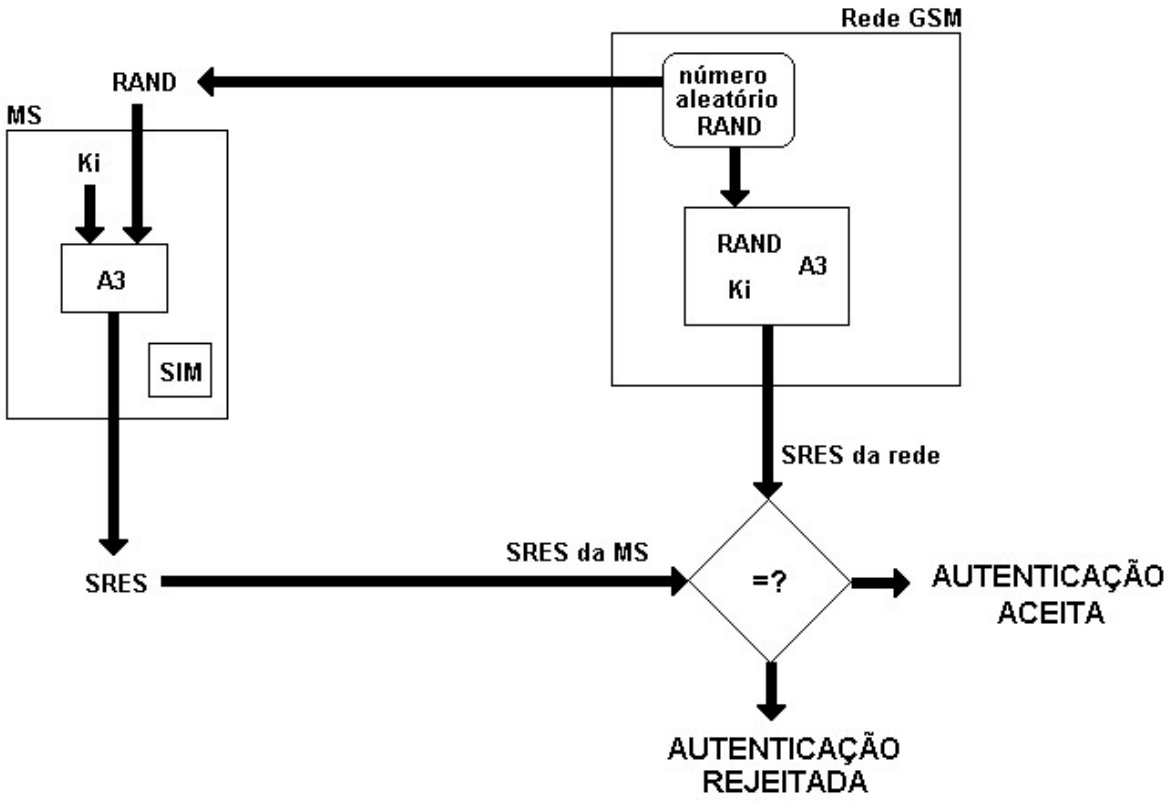
Objetivo da Autenticação do Assinante:

- proteger a rede contra o uso não autorizado e garantir que é o assintante correto que está utilizando a conta, previnindo, assim, ataques mascarados.

O algoritmo de autenticação é conhecido como **A3** e é implementado no Centro de Autenticação (AuC) e no SIM. O método empregado entre a AuC e o SIM é o mecanismo desafio/resposta utilizando números randômicos.

♦ Processo de Autenticação do Sistema GSM

GSM
GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS



- A autenticação no modelo GSM funciona em outros países além do país de registro do MS, porque a rede local pergunta para a **HLR** (Registro de Localização) da rede "natal" do assinante o valor de **Ki** necessário para a autenticação. O **HLR** também é responsável por saber a localização do MS a todo momento.

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- ***(3) Ciframento***

  - garante a segurança no nível de conexão na troca de mensagens entre os MSs e as estações rádio base.

Objetivo do Ciframento:

- assegurar a privacidade das informações do usuário que são transmitidas nos canais de comunicação, assim como informações de sinalização.

O algoritmo de ciframento é conhecido como **A5** e está contido nos equipamentos móveis (MS) e nas estações de base. O **A5** pode ser implementado em *hardware* utilizando por volta de 3000 transistores.

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- ***Algoritmos de Segurança do Sistema GSM***

A3 – Algoritmo de Autenticação

- tem a função de gerar a resposta **SRES** para mecanismo de desafio/resposta.
- utiliza a chave secreta **Ki** e o parâmetro **RAND**, ambos de 128 bits.
- a base do A3 é o algoritmo COMP128. O COMP 128 gera uma resposta de 128 bits, mas como o **SRES** possui apenas 32 bits, são utilizados apenas os primeiros 32 bits da saída do COMP128.

A8 – Algoritmo Gerador de Chaves

- gera a chave de sessão (**Kc**) que é composta de 64 bits.
- o A8 também se baseia no COMP128.

A5 – Algoritmo de Criptografia

- é um cifrador de cadeia de valores (*stream cipher*) usado para encriptar a transmissão de dados pelo ar. A entrada do algoritmo é a chave de sessão (**Kc**) e o quadro que está sendo cifrado.
- o **A5** original foi considerado muito forte para a exportação. Outras implementações mais fracas como o **A5/1** e o **A5/2** surgiram. A versão do algoritmo denominada **A5/0** não executa nenhum ciframento.
- a complexidade do **A5/1** é da ordem de 2^{54}, enquanto que a complexidade do **A5/2** é da ordem de 2^{16}. O **A5/2** é utilizado nos EUA.

A38 – Algoritmo simplificado que executa as funções do A3 e do A8

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- ***Módulo de Identificação do Assinante (SIM Card):***

  - Trata-se de um *smart card* que contém todas as informações e algoritmos necessários para autenticar o assinante na rede.

    - Tamanho padrão 25mm x 15mm.

    - É composto de três tipos de memória:

    ROM ➔ usada para armazenar o **S.O.** do cartão e os algoritmos **A3** e **A8**.

    RAM ➔ usada para a **execução dos algoritmos** e para a **transmissão dos dados**.

    EEPROM ➔ usada para armazenar o resumo dos **números discados**, **agenda telefônica**, a chave secreta **Ki**, **IMSI** (identidade móvel internacional do assinante) e as informações da rede **TMSI** (identidade móvel temporária do assinante) e **LAI** (identidade de localização da área). Armazena o **PIN**.

Exemplo de um SIM Card

♦ Modelo de Segurança GSM

GSM®
GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- ***Módulo de Identificação do Assinante (SIM Card):***

- O acesso ao SIM é controlado por um Número de Identificação pessoal (PIN), que é livremente escolhido entre 4 a 8 dígitos, podendo ser alterado pelo usuário do equipamento móvel.

- Se o usuário tentar acessar o SIM por três vezes utilizando um PINs errados, ele somente poderá ser desbloqueado através de um número de 8 dígitos chamado chave de desbloqueio (PUK). O SIM é permanentemente bloqueado após dez erros consecutivos da sua entrada.

- O número PIN2 é utilizado para permitir a alteração dos campos de dados do SIM (informaçõs de acesso à rede, número do telefone, etc). Ele não pode ser errado mais que três vezes, caso contrário deve-se utilizar o PUK para desbloqueá-lo.

Exemplo de um SIM Card

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- ***Possíveis ataques ao Sistema GSM***

Apesar da interceptação de mensagens no ar e a decodificação em tempo real de uma chamada telefônica ainda ser impossível, existem algumas especulações de possíveis métodos de atacar a rede GSM em seus pontos fracos.

1) Ataque por força bruta sobre o algoritmo A5

- Utilizando um Pentium III de 600MHz com aproximadamente 20 milhões de transistores seria possível a implementação de 10.000 algoritmos A5/1 em paralelo em um único chip, possibilitando a geração de 2M chaves por segundo por A5/1. Considerando o espaço chaveado de 2^{54} possibilidades de chaves seriam necessárias 250h para encontrar a chave com um único chip. A utilização de múltiplos chips em paralelo poderia reduzir esse tempo drasticamente.

2) Ataque de divisão e conquista sobre o algoritmo A5

- Esse ataque tenta reduzir a complexidade do ataque da força bruta de 254 para 245 (redução de 512 vezes) baseando-se no fato do “conhecimento do texto cifrado”. Esse “conhecimento” tenta “chutar” os bits do cabeçalho dos quadros transmitidos. Existem alguns ataques baseados em equações lineares para a quebra do algoritmo A5/1.

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

3) Ataque por invasão à rede

- A criptografia é utilizada apenas nas transmissões pelo ar, isto é, entre o MS e a estação radio base (BTS). Após a BTS, a mensagem é transmitida sem qualquer segurança criptográfica através das operadoras da rede, utilizando transmissões cabeadas, microondas ou até mesmo via satélite.

4) Ataque através da obtenção da chave a partir do SIM

- A segurança de toda rede GSM está baseada na chave secreta **Ki**. Se a integridade da chave for comprometida, então a conta do usuário também estará comprometida.
- Esse ataque é baseado em uma abertura do algoritmo COMP128 que revela informações sobre o **Ki** quando um número **RAND** apropriado é enviado como argumento para o algoritmo **A8**. A SIM pode ser acessada através de um *smartcard* concectado a um PC que executa cerca de 150.000 tentativas e consegue deduzir a chave secreta aplicando algoritmos de criptoanálise.
- Esse tipo de ataque requer cerca de 8 horas para sua execução total.
- Contudo, o sistema GSM é dotado de uma função que detecta se dois telefones com a mesma identificação estão sendo utilizados simultaneamente, registrando a ocorrência e notificando o usuário do aparelho celular.

♦ Modelo de Segurança GSM

GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

5) Ataque por obtenção da chave a partir do SIM pelo ar

- O ataque ao SIM pode ser realizado pelo ar utilizando-se um equipamento que bombardeia o MS com desafios/resposta com o intuito de reconstruir a chave secreta a partir das respostas.
- Estipula-se que um ataque como esse pode ser realizado entre 8 e 13 horas.
- Esse ataque pode ser realizado dentro do metrô, onde o sinal da estação radio base (**BTS**) legítimo não está disponível.
- O usuário do celular deve ficar atento ao fato desse ataque provocar a queda rápida da carga da bateria do aparelho celular.
- O *hacker* pode executar o ataque durante 20 minutos diariamente enquanto o usuário do aparelho executa seu trajeto em direção ao trabalho.
- A partir do momento que o SIM está clonado, o clone poderá ser utilizado nos momentos em que o SIM original não está acessando a rede até que o usuário receba um novo SIM da rede GSM, o que na prática não ocorre.

6) Ataque por obtenção da chave a partir da AuC

- O mesmo ataque utilizado para obter a chave a partir do SIM pode ser utilizado para obter a chave secreta **Ki** a partir do **AuC** (Centro de Autenticação da **BTS**). A diferença é que a **AuC** é muito mais rápida que o SIM para processar os dados.
- A segurança do **AuC** não é publicada, por isso não pode ser analisada em detalhes.

♦ Modelo de Segurança GSM

GSM®
GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

7) Ataque sobre o algoritmo A8

- Um ataque sobre o algoritmo gerador de chaves A8 permite ao *hacker* descobrir a chave secreta (**Ki**) baseada no desafio/resposta **RAND**, a chave de sessão (**Kc**) e a resposta **SRES**, assumindo que o algoritmo utilizado para o A3 e o A8 sejam baseados no COMP128.

- Encontrando-se um número **RAND** e o **SRES** no ar, visto que o envio dos mesmo não é criptografado, a chave **Ki** pode ser deduzida através desses números e a chave de sessão **Kc** pode ser deduzida pelos quadros cifrados.

♦ Resumo dos aspectos de segurança dos sistemas AMPS, USCD e GSM

	AMPS	USCD (IS-95 e IS-136)	GSM
Mecanismo de autenticação	Baseado no uso de parâmetros armazenados dentro da estação móvel e que são transmitidos pelo ar sem nenhuma proteção. Processo que coloca em risco a segurança do sistema.	Procedimento desafio/resposta, no qual os parâmetros de identificação não são transmitidos pelo ar, por tanto não coloca em risco a segurança do sistema.	Procedimento desafio/resposta, no qual os parâmetros de identificação não são transmitidos pelo ar, por tanto não coloca em risco a segurança do sistema.
Mecanismo de privacidade	Não tem.	Usa criptografia para proteção dos dados e da sinalização trafegados entre o assinante e a rede.	Usa criptografia para proteção dos dados e da sinalização trafegados entre o assinante e a rede.
Mecanismo de proteção da identidade e localização do assinante	Não tem.	Não tem.	Usa criptografia e procedimentos de identificação temporal.
Facilidade de interceptação e decodificação dos sinais de RF	Fácil. *Scanners* que rastreiam e interceptam sinais analógicos são fáceis de construir ou comprar.	Difícil. Usa canal digital difícil de ser demodulado e decodificado por *scanners* simples.	Difícil. Usa canal digital difícil de ser demodulado e decodificado por *scanners* simples.
Utilização de algoritmos de criptografia	Não utiliza.	Usa algoritmos de chave privada, os quais estão severamente protegidos por leus de *Copyright*, portando de acesso restrito.	Usa três algoritmos de chave privada denominados A3, A8 e A5. Este último é um *stream cipher*, apoiado por mecanismos de camada física. Estes algoritmos têm acesso restrito.
Parâmetros de entrada ou chaves para os algoritmos de criptografia	Não tem.	A-Key é de 64 bits. Desconhece-se o tamanho de chave dos algoritmos.	Ki, RAND são de 128 bits, e o Kc tem 64 bits. Parte do algoritmo A5 foi publicada na *Internet*, o tamanho é 40 bits. Desconhece-se o tamanho dos demais algoritmos.
Método de disponibilização da chave	Não tem.	A chave A-Key é enviada pela operadora ao assinante por correio convencional. O qual é armazenado na Estação Móvel de forma manual e nunca é transmitida pelo ar.	A chave Ki já vem embutida no SIM e nunca é transmitida pelo ar.

♦ Padrões e Tecnologias

IEEE 802.16

- Autenticação
- Associações de segurança
- Perfil de certificado X.509
- Autorização PKM
- *Privacy and management key*
- Encriptação

♦ Padrões e Tecnologias

IEEE 802.16 - Autenticação

- Reúso das tecnologias de segurança das redes cabeadas

- Autenticação
  * A estação assinante (SS) busca uma estação base (BS)
  * SS configura os parâmetros PHY de acordo com a BS
  * SS cria canal para estabelecimento da conexão
  * O protocolo PKM (*Privacy and Key Management*) da BS autoriza a SS
  * SS solicita conexão
  * BS envia uma *connection ID* para a conexão secundária de gerência
  * A partir daí, BS e SS criam conexões de transporte

♦ Padrões e Tecnologias

IEEE 802.16 – Associações de Segurança

- Associações de segurança (SA) mantém o nível de segurança uma conexão

- O padrão idendifica 2 tipos de SA, mas define apenas *data SA*

- Características
  - * Um SAID de 16 bits
  - * Um cifrador usado na autenticação (DES)
  - * 2 Chaves de encriptação de tráfego (TEK)
  - * TEK *timelife* (30 min. A 7 dias)
  - * VI de 64 bits

♦ Padrões e Tecnologias

IEEE 802.16 – X.509

- Identifica as partes na comunicação

- X.509 versão 3: RSA + SHA1

- Características
  * Chave pública da comunicação
  * Algoritmo de assinatura

- Tipos de certificado
  * Certificado de SS
  * Certificado do fabricante

♦ Padrões e Tecnologias

IEEE 802.16 – Autorização PKM

- Protocolo de Autorização

```
Mensagem 1:
SS → BS Cert(Fabricante(SS))
Mensagem 2:
SS → BS Cert(SS) | Capacidades | SAID
Message 3:
BS → SS RSA-Encrypt(PubKey(SS), AK) |
Lifetime | SeqNo | SAIDList
```

- Tipos de certificado
  - * Certificado de SS
  - * Certificado do fabricante

♦ Padrões e Tecnologias

IEEE 802.16 – PKM

- Estabelece uma *data SA* entre SS e BS

```
Mensagem 1:
BS → SS:SeqNo | SAID | HMAC(1)]
Message 2:
SS → BS:SeqNo | SAID | HMAC(2)
Message 3:
BS → SS:SeqNo | SAID | OldTEK |NewTEK |HMAC(3)
```

- 3DES na cifragem das TEKs
  * DES com até 3 chaves de 56 bits aplicadas

♦ Padrões e Tecnologias

IEEE 802.16 – Encriptação

- DES-CBC (Data Encryptation Standard - *Electronic Code Book*)

- Opera sobre o *payload* e o texto limpo do MPDU

- Cálculo do VI é dado por XOR entre
  * Campo de sincronização do mais recente GMH
  * SA IV

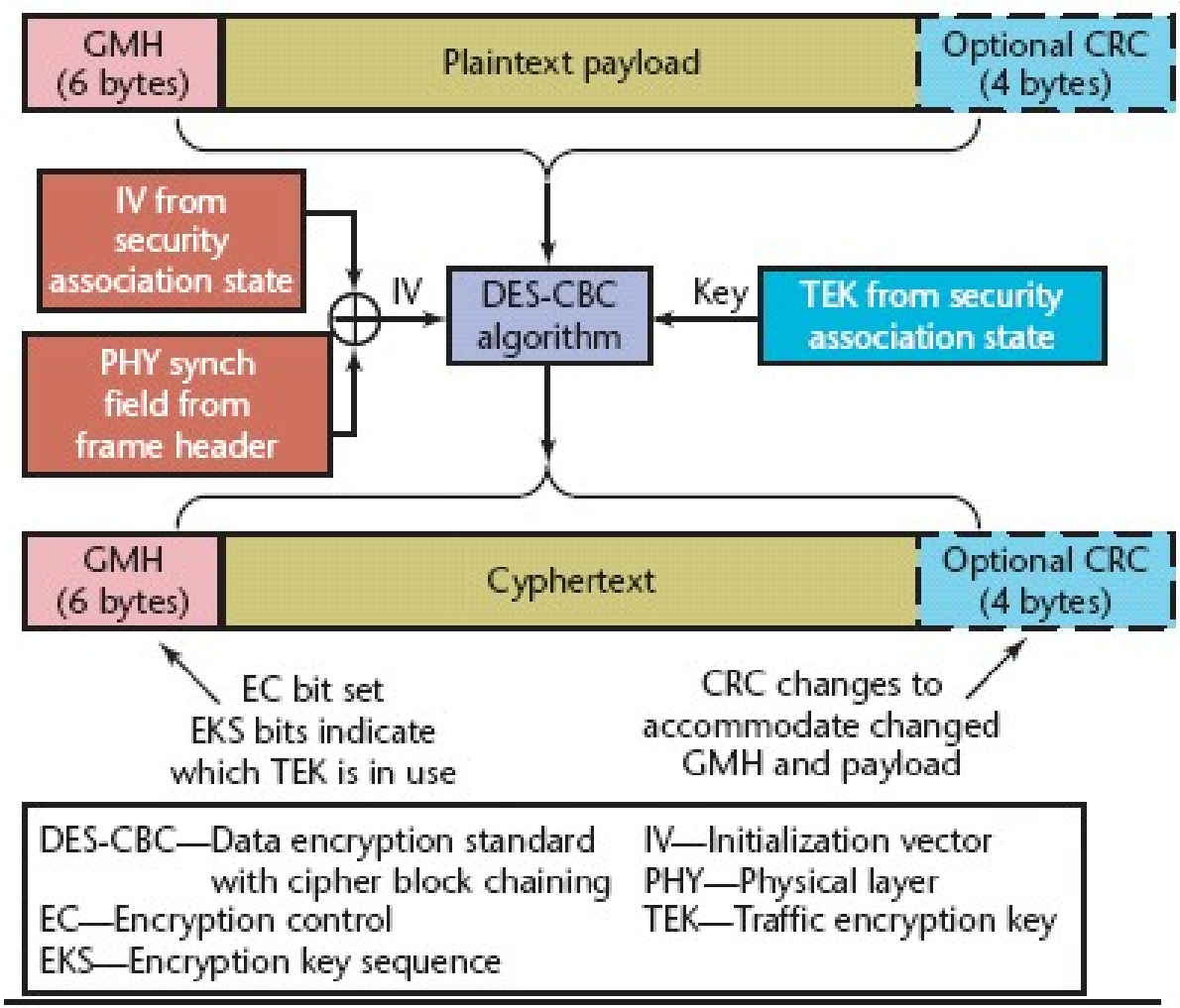


Figure 2. IEEE 802.16 encryption process. The Data Encryption Standard in cipher block chaining mode enciphers the multiprotocol data units but not the MPDU generic MAC header or the cyclic redundancy checking.

♦ *A "latinha" que escuta...*

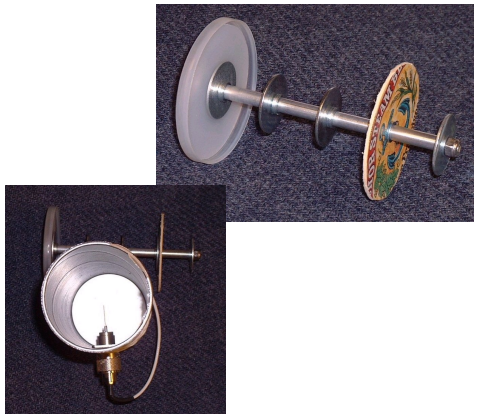
• ***Teste de segurança da revista INFO Exame (jun/2002)***

- Região central de São Paulo onde há grande concentração de escritórios (Av. Paulista/ Av. Faria Lima)

- Foram utililizados: um notebook, um cartão PCMCIA, uma antena artezanal e o softaware livre *NetStumbler*

- Foram detectadas **43** redes sem fio (802.11b), das quais **35** estavam desprotegidas (sem nenhum tipo de criptografia), sendo que o padrão de rede permite ativar o sistema de proteção criptográfica sem maiores dificuldades

- O alcance do "kit" é de 16*Km* (área livre)



♦ *A "latinha" que escuta...*

- "*Cantenna*"

http://www.cantenna.com/

- Dimensionando a "latinha":

http://www.turnpoint.net/wireless/cantennahowto.html

3.25 **Can Diameter** Calculate

Cuttoff Frequency in MHz for TE11 mode		MHz
Cuttoff Frequency in Mhz for TM01 mode		MHz
Guide Wavelength in Inches		inches
1/4 Guide Wavelength		inches
3/4 Guide Wavelength		inches

♦ Conclusões

- Redes sem fio já oferecem alguma confiabilidade
- Técnicas criptográficas com chaves maiores têm sido adotadas
- Redes celulares são exemplo
- Questões ligadas a redes *ad-hoc* e *mesh* tem poucas opções
- Os administradores, por diversas vezes, subutilizam a tecnologia

rsalustiano@gmail.com

tnunes@gmail.com